(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 560 100 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
03.08.2005 Bulletin 2005/31

(51) Int Cl.[7]: **G06F 1/00**

(21) Application number: **05100336.6**

(22) Date of filing: **20.01.2005**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU MC NL PL PT RO SE SI SK TR
Designated Extension States:
AL BA HR LV MK YU

(30) Priority: **29.01.2004 US 767884**

(71) Applicant: **Novell, Inc.**
Provo, Utah 84606-6194 (US)

(72) Inventors:
- **Burch, Lloyd Leon**
  Rayson, UT 84651 (US)
- **Earl, Douglas G.**
  Orem, UT 84097 (US)
- **Carter, Stephen R.**
  Spanish Fork, UT 84660 (US)

(74) Representative: **Hanna, Peter William Derek et al**
Hanna, Moore & Curley
11 Mespil Road
Dublin 4 (IE)

(54) Techniques for establishing and managing a distributed credential store

(57) Methods and systems are provided for establishing and managing a distributed credential store. An identity service (410) aggregates identity information from one or more identity stores and maintains the information as a remote credential store (303,411). Initially, the remote credential store, or portions thereof, is transmitted to a principal service (420) as an initial configuration of a local credential store (302,425). A principal interacts with the principal service for defining or modifying a policy that identifies portions of the remote credential store which are to be synchronized with the local credential store. In some embodiments, the principal interacts with the principal service for defining a local policy that identifies portions of the local credential store (302) which are not synchronized with the remote credential store (303). The interactions between the credential stores are trusted and secured.

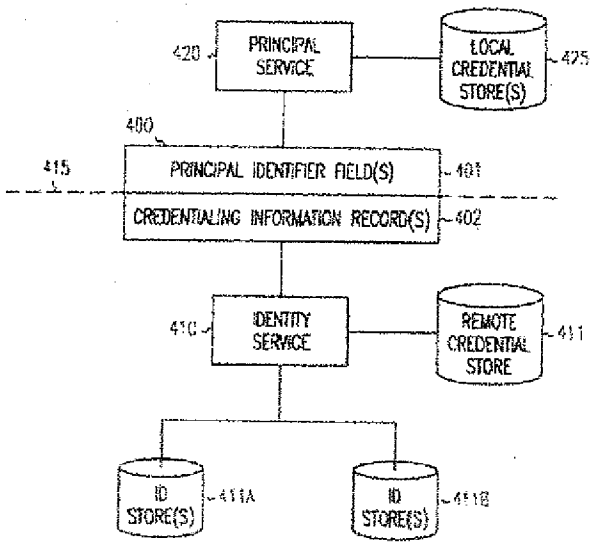

FIG. 4

EP 1 560 100 A1

Description

Field of the Invention

[0001] The invention relates generally to network security, and more specifically to techniques for establishing and managing a distributed credential store.

Background of the Invention

[0002] As individuals continue using the Internet for connecting to a myriad of services and resources, a variety of confidential information and identity information about those individuals needs to be managed, synchronized, and securely distributed. In many instances, this information is concurrently and manually managed in environments local to the individuals, in local enterprise environments associated with the individuals, and in environments that are local to the services and resources.

[0003] Having the identity and confidential information housed and managed in a variety of environments presents a number of challenging problems. For example, individuals are not always properly authenticated into their enterprise environment, which means that access to some information may not be available to individuals who use different computing devices from time to time and who are not properly logged into their appropriate enterprise environments from time to time. Additionally, management of the identity and confidential information usually occurs in multiple environments. That is, an individual maintains some information, the enterprise maintains other information, and the services or resources maintain still other information. In some cases, the same information is separately managed in duplicate. This creates synchronization problems for the individuals and for network administrators.

[0004] Furthermore, the information, as it is being managed and manually maintained or utilized, becomes unduly exposed during network transmissions. This means that each time portions of the information are transmitted for purposes of authentication or for purposes of synchronization it can become compromised and intercepted. This results in a variety of security issues which must be established for network interactions that involve the transfer of the information.

[0005] Typically, security measures will entail establishing trust relationships utilizing public- private key pairs with encryption and the like. The encryption is used in secure communications for minimizing exposure to confidential information and identity information. However, mobile individuals may not have static key pairs with services and may often use a laptop to connect from a variety of Internet Service Providers (ISPs), such that the individuals do not have static Internet Protocol (IP) addresses which can uniquely and securely establish the needed trusted relationships between the individuals and other services or resources. Consequently, individuals are often limited in their use of or prohibited in their use of certain confidential and identity information in many contexts when adequate security measures are enforced in conventional manners.

[0006] Thus, even the most elaborate conventional techniques that attempt to automate and synchronize an individual's confidential information and identity information still falls short of providing a consistent level of sustainable service, because in many cases the user is unable to effectively access some of his/ her needed information.

[0007] Thus, there is a need for establishing and managing a distributed credential store, where that credential store can be securely accessed, better managed, and consumed in order to provide an improved level of consistent service.

Summary of the Invention

[0008] The present invention provides methods and systems for establishing and managing a distributed credential store, in accordance with claims which follow. In various embodiments of the invention, techniques are presented for establishing and managing a distributed credential store. An identity service interacts and manages one or more identity stores associated with a principal. The identity service and the principal interact according to a trust specification, such that all communications are secure. Initially, the identity service creates an initial configuration instance of a distributed credential store for the principal according to a synchronization policy which is created and maintained by the principal. The synchronization policy defines fields of a remote credential store which are to be kept in synch with a local credential store.

[0009] The local credential store is managed by the principal in a processing environment that is local to the principal. The identity service generates a remote credential store which it maintains to synchronize records of the local credential store with affected records of the one or more identity stores. The synchronization is driven by the synchronization policy.

[0010] If the principal falls out of communicatio n with the identity service and subsequently re- establishes communication, then the identity service uses the synchronization policy communicated from the principal to generate a new active instance of the remote credential store and bring the principal's local credential store and the remote credential store into synch with one another according to the synchronization policy. The principal can maintain personal entries in the local credential store which are not communicated to and synchronized by the identity service into the remote credential store.

Brief Description of the Drawings

[0011]

FIG. 1 is a flowchart representing a method for man-

aging a distributed credential store;

FIG. 2 is a flowchart representing another method for managing a distributed credential store;

FIG. 3 is a diagram of a distributed credential management system; and

FIG. 4 is a diagram representing a distributed credential store.

Detailed Description of the Invention

[0012] In various embodiments of the invention, the term " principal" is used. A principal is an electronic representation of an entity. An entity can be a resource, a user, an agent, an application, a system, a service, a group, a department, an object, etc. An entity consumes information, provides information, or provides a service to other entities over a network. Moreover, an entity can perform combinations of the above-mentioned operations.

[0013] In one embodiment, the term principal is consistent with how that term is generally understood in the security arts. For example, the term principal can be used in the context of Security Assertion Markup Language (SAML) which is an extension of the Extensible Markup Language (XML). SAML is used for securely processing assertions about a user or application (e. g., principal). More recently, SAML has been extended with technology referred to as Liberty. Liberty is part of the Liberty Alliance Project (LAP) and is attributed to open interoperable standards for federated network identities. Thus, the term principal can also be used in the context of Liberty technologies.

[0014] A SAML encoded statement includes an assertion, a protocol, and a binding. There are generally three types of assertions: an authentication assertion used to validate a principal's electronic identity, an attribute assertion that includes specific attributes about the principal, an authorization assertion that identifies what the principal is permitted to do (e. g., policies). The protocol defines how a SAML processing application will ask for and receive the assertions. The binding defines how SAML message exchanges are mapped to Simple Object Access Protocol (SOAP) exchanges, or other protocol exchanges.

[0015] In general terms, SAML techniques improve security between business- to-business (B2B) electronic transactions and business- to- customer (B2C) electronic transactions. The techniques permit one principal to log in with a single transaction to a receiving principal and then use a variety of the receiving principal's disparate services by providing the SAML statements when needed. SAML techniques are not limited to inter- organization relationships (e. g., B2B or B2C); the techniques can be used within a single organization (intra-organization). SAML techniques are supported with a variety of network protocols, such as Hypertext Transfer Protocol (HTTP), Simple Mail Transfer Protocol (SMTP), File Transfer Protocol (FTP), SOAP, BizTalk, and Electronic Business XML (ebXML). The Organization for the Advancement of Structured Information Standards (OASIS) is the standards group for SAML. The techniques of Liberty are enhancements to the SAML techniques and may also be used in connection with various embodiments of this invention. However, it is to be understood that SAML and Liberty techniques are not needed to perform the teachings of all embodiments of the invention. These techniques complement some embodiments of this invention. In this sense, the integration of SAML and Liberty techniques with some of the embodiments presented herein is intended to be part of certain aspects of this invention, but not all embodiments of this invention are dependent on SAML or Liberty technology. In a similar manner there are various other existing authentication techniques that may be practiced in connection with some embodiments of this invention. But, once again these other authentication techniques are not necessary for realizing the benefits of all embodiments of the invention. Some of these techniques include Public Key Infrastructure (PKI) techniques including public- private key pairs, digital certificates, biometric authentication, or use of conventional identifications and passwords.

[0016] A credential store is a file, database, directory, or combinations of the same which house(s) confidential information and identity information about one or more principals. The confidential information is defined by attribute fields that identify a type of confidential data; each attribute field is populated with specific attribute values which identify the values associated with confidential data. A credential store also includes identity/ authentication information and or authentication techniques or services associated with authenticating principals vis-à-vis other principals. In some cases the identity information is a legacy identification and password pair. In other cases, the identity information is a certificate or an assertion, such as a SAML or Liberty assertion that identifies what identity information is needed to authenticate and how that authentication is to take place.

[0017] The credential store also includes policies that define how attributes can or cannot be processed in a given principal- to- principal relationship. The authentication information, authentication techniques/ services, attributes, and policies combine to form credentialing information records that populate the credential store. Furthermore, a credential store need not reside contiguously within storage or memory. That is, a credential store can be logically assembled from a variety of other identity stores residing in a plurality of remote storage and memory locations.

[0018] A distributed credential store is one that is maintained locally from within a local environment of a principal, but incorporates and synchronizes in whole or

in part with a remote credential store. A single distributed credential store can be associated with a single principal. Alternatively, a single distributed credential store can be used to manage a plurality of principals. In this latter embodiment, each entry within the distributed credential store is uniquely encrypted for a particular principal's use.

[0019] Various embodiments of this invention can be implemented in existing network products and services. For example, in some embodiments, the techniques presented herein are implemented in whole or in part in the iChain ®, Border Manager ®, and Excelerator ® products distributed by Novell, Inc., of Provo, Utah. Of course, the embodiments of the invention can be implemented in a variety of architectural platforms, systems, or applications. For example, portions of this invention can be implemented in whole or in part in any distributed architecture platform, operating systems, proxy services, or browser/ client applications. Any particular architectural layout or implementation presented herein is provided for purposes of illustration and comprehension only and is not intended to limit aspects of the invention.

[0020] FIG. 1 is a flowchart representing one method 100 for managing a distributed credential store. The method 100 is implemented as one or more applications or services which reside in a computer- accessible medium and is accessible over a network. Some portions of the processing of the method 100 (hereinafter "processing") operates in an external computing environment from a principal while other portions of the processing operates in a local computing environment of the principal. The two processing portions are interfaced using any existing or customized protocols and application programming interfaces (APIs). In some embodiments, a principal's local processing interfaces with the external processing via a World- Wide Web (WWW) browser operating within a client of the principal. A client is a processing device from which the browser is operating on. Initially, an identity service is in a trusted relationship with one or more identity stores that house attribute and identity information about one or more principals. The identity service is capable of authenticating a principal and establishing a secure communication with that principal vis-à-vis other different principals with which the principal may interact. In some cases, that secure communication entails the identity service encrypting communications and signing communications with public- private key pairs. The principal via a client service can decrypt the communications using its own private key and a public key associated with the identity service.

[0021] A sample technique for secure and trusted relationships between a principal and an identity service can be found in our co-pending European patent application no. 04106396.7 entitled " Techniques for Dynamically Establishing and Managing Authentication and Trust Relationships "

[0022] Information and transactions that the principal can send and receive from the identity service may exist in global policies defined in a trust specification between the identity service and the principal. The trust specification can be managed, owned, and controlled by appropriate network administrators and modified as needed to enable or disable features of the present invention. The trust specification will also dictate the type of secure communications and methods used during interactions between the identity service and the principal. In some cases, the identity service and the principal can communicate with one another via SAML or Liberty assertions and their associated protocols. The trust specification also ensures that communications about a credential store are secure and verifiable in order to maintain proper security.

[0023] Initially, the principal desires to establish an initial instance of a distributed credential store. This entails creating a local credential store and a remote credential store and a policy that will drive the synchronization between the local and remote credential data stores. The interaction between the local and remote credential store and the results that it produces in the local credential store is an instance of the distributed credential store.

[0024] One way to create an initial instance of the distributed credential store is for the principal to request the initial instance (pull) from the identity service. Another way to create an instance is for the identity service or some other third- party to independently request or generate an instance of the distributed credential store for a particular princ ipal (push). Thus, an initial instance of a distributed credential store can be generated or created from either a push or pull model.

[0025] Once a push or pull request is initially received, the identity service validates that the request is permissible and if it is generates an initial instance of a distributed credential store. In one embodiment, the identity service generates the initial instance by inspecting a global contract associated with a particular principal and by inspecting the appropriate trust specification and global policies. The global contract defines how a principal is authenticated to various other principals using specific identifying information. The global contract also provides information that permits the identity service to acquire appropriate attribute information for a given relationship of the principal vis-à-vis other principals.

[0026] The global policy may restrict certain relationships based on physical locations, time limitations, calendar day limitations, or specific predefined events which limit certain relationships. The global contract identifies the specific identity stores which house the needed information needed by the identity service in order to construct an initial instance of the distributed credential store. The trust specification identifies how the identity service and the principal will communicate with one another about the distributed credential store in order to satisfy themselves that each communication is secure and trusted.

[0027] Once the global contract, global policy, and trust specification are inspected and evaluated, records associated with the distributed credential store are generated and either batched until entirely assembled or streamed individually as assembled using the secure communications defined in the trust specification directly to the principal. Each record includes a particular relationship between a principal vis-à-vis another principal and includes authentication information, authentication techniques/services, attributes, and policies. The authentication information and authentication techniques/ services are used to authenticate the principal to another principal defined in the record. In some cases, the authentication information and authentication techniques/ services are represented as a certificate, and can be optionally provided as a SAML or Liberty assertion. The attribute information identifies confidential information that can be accessed or not accessed during the relationship defined by the record. Policies are also included in the record that identifies the operations which are permissible or not permissible against the attributes during a relationship defined by the record. Each record can be viewed as a credential for a particular principal- to-principal relationship.

[0028] The description presented above provides the context with which a distributed credential data store is initially established, configured, and communicated to the local environment of a principal. Once this initial configuration is received it is established as a principal (local) credential store by the principal.

[0029] The records established by the identity service form an enterprise credential store, which is maintained and managed by the identity service in concert with the principal credential store. Accordingly, at 110, portions of the enterprise credential store are associated or linked by the identity service to appropriate portions of the principal credential store, which is managed by a principal service of the principal. In one embodiment, at 111, the identity service selectively aggregates or maintains metadata such as links associated with one or more records of appropriate identity stores as defined by a policy or contract associated with the principal. The identity service can maintain contents of selective identity records or maintain links to the selective identity records of appropriate identity stores. These duplicated records or maintained links form the enterprise credential store which the identity service manages.

[0030] The identity service is configured to detect when changes to the duplicated records or maintained links are made in the identity stores via a data store event that is trapped and monitored by the identity service. Thus, if an administrator alters a record of an identity store that the identity service is tracking as part of the enterprise residential store, the identity service is in a position to acquire the changes and transmit, at 112 the changes to the principal credential store, if desired.

[0031] The principal via its principal service communicates an initial synchronization policy to the identity service. With this synchronization policy, both the identity service and the principal service know which portions of the enterprise credential store and the principal credential store are to be selectively synchronized with one another, as depicted at 120.

[0032] The synchronization policy can be maintained by the principal service of the principal. This has the added benefit of permitting the principal service and the identity service to synchronize after an initial configuration of the distributed credential store has been instantiated for a principal but where the principal drops out of communication with the identity service for some period of time. For example, suppose that a principal acquires an initial principal credential store from the identity service and the identity service generates an active enterprise credential store related to the principal credential store.

[0033] Now suppose that the principal logs off of or terminates communication with the identity service for some extended period of time and then at a later time reestablishes communication with the identity service. The principal will have a principal credential store which may or may not have been modified during the lapse of non communication, and in a similar manner one or more records that were previously associated with an active enterprise credential store may have changed during the period of non communication within one or more affected identity stores. The identity service can automatically generate a new up- to- date instance of a needed enterprise credential store and synchronize with any modified principal credential store via the principal's local synchronization policy which the principal communicates during initial re- communication to the identity service. If there are conflicts between changes of the personal credential store and the newly instantiated enterprise credential store, the conflicts can be resolved by the policy.

[0034] The principal, in some embodiments, may desire to maintain some personal credential information associated with private business or affairs of the principal separate and distinct from the management of the enterprise credential store. In these embodiments, at 121, the principal can selectively insert this personal credential information into the principal credential store where it is maintained and managed by the principal service of the principal. However, if this personal information is defined by a local synchronization policy of the principal as information that is not to be synchronized with the enterprise credential store, then, at 122, the enterprise credential store is prevented from acquiring or synchronizing with this personal credentialing information.

[0035] Conversely, some new or modified identity information can be inserted or changed by the principal within the principal credential store, at 123, and according to the synchronization policy automatically communicated to the identity service and updated to the enterprise credential store. An update to the enterprise cre-

dential store will force the identity service to update the effected records in the appropriate identity stores.

[0036] In a like manner, at 124, if the synchronization policy dictates, any changes detected in the enterprise credential store will generate automatic updates to the appropriate records of the principal credential store.

[0037] All interactions between the enterprise credential store and the principal credential store occur according to the strictures of the overall trust specificatio n between the identity service and the principal. Accordingly, at 130, all conflicts and communications are maintained in conformance with the trust specification and the overall global policies and contracts held between the identity service and the principal.

[0038] Moreover, the principal via the principal service can alter the synchronization policy and communicate the changes to the identity service at 132. This permits the principal to control what is and what is not synchronized. Of course, in some embodiments, a global policy or contract associated with the principal at the identity service level can constrain what portions of the policy which can be modified and driven by the principal.

[0039] Embodiments of method 100 demonstrate how a principal can interact with an identity service for purposes of managing and controlling its own version of a credential store. This principal credential store can be encrypted and maintained in a local environment of the principal or on a client processing device of the principal. Each time the principal re- establishes communication with the identity service, the principal's synchronization policy can be used to re- synchronize the principal credential store with an identity service generated enterprise credential store. This permits a principal to move around and independently access needed credentialing information to successfully interact with other principals. It also permits the principal to maintain some information which is never synchronized to the enterprise or known to the enterprise. Moreover, no communication between the principal credential store and the enterprise credential store occur outside of trusted communications defined by a trust specification.

[0040] FIG. 2 is a flow diagram of another method 200 for managing a distributed credential store. The method is implemented in a computer readable medium and is accessible over any network. The processing of the method 200 (hereinafter "processing") represents processing performed by a client or principal service that interacts with an identity service. In one embodiment, the interface between some portions of the processing and the identity service is implemented within a WWW browser. In some embodiments, the processing is a service that manages a local credential store on behalf of multiple principals that interact with the identity service, in this sense the local credential store can logically represent multiple unique principal credential stores as discussed above with FIG. 1. At 210, the processing establishes and initiates a trusted and secure relationship with a remote credential store via an identity service. The identity service has access to one or more identity stores associated with one or more principals. The identity service logically assembles a remote credential store from the one or more identity stores on behalf of the processing. The remote credential stores includes one or more enterprise credential stores similar to what was discussed above with respect to FIG. 1. The trust relationship between the generated remote credential store and the processing is defined and driven by a trust specification as depicted at 211.

[0041] At 220, the processing receives changes associated with one or more entries in the remote credential store into the local credential store. That is, a synchronization policy informs the identity service as to which records or entries associated with whole records or portions of records included within the remote credential store which are to be automatically communicated to the processing and updated to the appropriate affected entries of the local credential store. For efficiency purposes, the processing can manage some portions of the local credential store from memory and some portions from storage as depicted at 221. Again, at 222, the entries that are synchronized into the local credential store and transmitted from the local credential store to the remote credential store are managed by a local synchronization policy which can be communicated in whole or in part to the identity service for purposes of managing the synchronization of the remote credential store.

[0042] In one embodiment, at 223, the processing manages the local credential store for multiple unique principals. This may be advantageous when a single local credential store is servic ing a plurality of principals within a local network. In these instances, each entry within the local credential store is uniquely associated with a particular unique principal. Moreover, in some embodiments, each unique entry can be uniquely encrypted in a manner such that only the associated principal knows the proper decryption algorithm. This permits the processing to securely service multiple principals from a single local credential store.

[0043] The local synchronization policy will permit the processing, at 224, to automatically communicate changes with entries in the local credential store to the remote credential store via its identity service. As was discussed with FIG. 1, some entries in the local credential store will remain private or personal to the local credential store and will therefore not be communicated to the remote credential store. Again, these personal entries will be defined in the local synchronization policy and are not communicated or known to the remote credential store via the identity service. Accordingly, at 225, the processing manages some personal entries in the local credential store which are independent of and not communicated to or synchronized with the remote credential store.

[0044] At 230, any detected changes to entries of the local credential store which are identified as entries

which the processing wants the remote credential store to synchronize with (via the local synchronization policy) are transmitted to the remote credential store via the identity service.

[0045] The processing of FIG. 2 permits one or more principals to establish and manage a local credential store which selectively synchronizes with a remote credential store. The principals may from time to time drop out of communication with an identity service having the remote credential store; however, the principals will still maintain and have direct access to the local credential store. The local credential store provides the principals with credentialing information that the principals can use to authenticate with and interact with other different principals. When the principals re-establish communications with the identity service, any changes which are desired to be synchronized with the remote credential store can be automatically synchronized via trusted and secure communications defined by a trust specification between the processing and an identity service of the remote credential store.

[0046] FIG. 3 is a diagram of a distributed credential management system 300. The distributed credential management system 300 is implemented in a computer readable medium and accessible over a network. In some embodiments, the distributed credential management system 300 implements the processing described above with respect to methods 100 and 200 of FIGS. 1 and 2, respectively. The distributed credential management system 300 includes a trust specification 301, a local credential store 302, and a remote credential store 303. The local credential store 302 resides in the local computing environment of one or more principals 330. In one embodiment, the local credential store 302 resides on a client of a particular principal 330. In another embodiment, the local credential store 302 resides within a local secure network that is accessible to multiple principals 330.

[0047] Conversely, the remote credential store 303 resides remotely and external to the local computing environment of the principal 330. It is accessible via a network 304. The remote credential store is logically assembled and associated with selective attributes and identity information about the principal 330 and acquired from or maintained from one or more identity stores.

[0048] The local credential store 302 and the remote credential store 303 interact with one another via the network 304 with secure communications defined by the trust specification 301. The synchronization between entries of the remote credential store 303 and the local credential store 302, and vice versa, are driven by synchronization policies 310 and 320.

[0049] The local credential store 302 includes a local synchronization policy 310 which drives and defines the remote synchronization policy 320. The principal 330 defines the local synchronization policy 310 by identifying entries from the remote credential store 303 which are to be automatically synchronized with entries of the local credential store 302. The principal 330 also defines entries or portions of the local synchronization policy 310 which are to be synchronized and not synchronized with the remote credential store 303. The entries or portions to be synchronized are communicated from the local synchronization policy 310 over the network 304 to the remote synchronization policy 320.

[0050] In some embodiments, after the principal 330 has been out of communication with the remote credential store 303 for any period of time and then re- establishes communication via the network 304, appropriate portions of the local synchronization policy 310 are immediately communicated to establish a new instance of the remote synchronization policy 320. This new instance of the remote synchronization policy 320 permits an identity service associated with the remote credential store 303 to generate a new and active instance of the remote credential store 303 and synchronize appropriate portions of the remote and local credential stores 303 and 302, respectively.

[0051] In one embodiment, the local credential store 302 services multiple principals 310 and is accessible via a server or service to each of the multiple principals 330. In this embodiment, the local credential store 302 manages each unique principal 330 with uniquely encrypted records; where each encrypted record is encrypted in a format only know to its associated principal 330. Thus, the distributed management system 300 can be used by a single principal 330 or by multiple principals 330 within a local network with one another.

[0052] FIG. 4 is a diagram of a distributed credential store 400. The distributed credential store 400 is implemented in a computer readable medium and is accessible over a network 415. The distributed credential 400 is logically assembled and coordinated over the network 415 and is represented within a local environment of one or more principals as one or more local credential stores 425 and represented external to the local environments as a remote credential store 411.

[0053] The distributed credential store 400 includes principal identifier fields 401 and credentialing information records 402. Each principal identifier field 401 is capable of housing a principal identifier value. Each unique principal identifier value is associated with credentialing information housed in the credential information record 402.

[0054] The credentialing information houses authentication information, authentication techniques/ services, attributes, and policies that define authenticatio n and interactions between a particular principal identified by a principal identifier value of a principal identifier field 401 vis-à-vis a different principal. In one embodiment, the authentication information and authentication techniques/ services defined in any particular credentialing information are represented as a certificate. In some cases, the certificate can be expressed as a SAML or Liberty assertion.

[0055] An initial instance of the distributed credential

store 400 is created or instantiated by an identity service 410 when requested from a principal service 420 (pull model) or when requested by a different principal on behalf of a particular principal (push model). Once an initial created instance of the distributed credential store 400 is established. It is managed within the local environments of the principals by the principal service 420 as one or more local credential stores 425. If the principal service 420 falls out of communication with the identity service 401 for any period of time, the identity service can re-synchronize the local credential store 425 as soon as communications are subsequently re-established between the identity service 410 and the principal service 420.

[0056] Synchronization occurs via a synchronization policy, which is managed and controlled by the principal service 420. This policy is communicated from the principal service 420 to the identity service 410 and permits the identity service 410 to generate active instances of a remote credential store 411. The remote credential store is managed by the identity service 411 and corresponds to those portions of the distributed credential store 400 that are defined in the synchronization policy which are to be synchronized in the local credential store 425.

[0057] The remote credential store 411 is assembled and locally linked to appropriate records housed in one or more identity stores 411A and 411B. When the identity service 410 detects that changes defined in the synchronization policy occur to records being tracked in the distributed credential store 400, these changes are communicated to the principal service 420 for update to the local credential store 425 or these changes are updated to the appropriate records of the one or more identity stores 411A and 411B (in cases where the changes are detected as occurring within the local credential store 425).

[0058] The principal service 420 also maintains a number of credentialing information records 402 in the local credential store 425 which are not communicated and synchronized to the remote credential store 411. This is useful when a particular principal is maintaining personal credentialing information which it does not desire the identity service 410 to know about or to manage.

[0059] All communications occurring between the principal service 420 and the identity service 410 are performed according to a trust specification which can be inspected and validated for each communication. This permits both the principal service 420 and the identity service 410 to satisfy their selves that communications are legitimate and authorized.

[0060] In some embodiments, the principal service 420 resides as a server application or service to multiple principals. In these embodiments, the local credential store 425 can be segmented into records associated with each unique principal being serviced, where sets of the records associated with any particular principal is encrypted in a format only known to that particular principal.

[0061] In one embodiment, a policy associated with a distributed credential store 400 may insist that any instance of the local credential store 425 be removed from a processing device of the principal 420. In these situations, the local credential store 425 is removed from the processing device when the principal 420 logs off of or terminates (normally or abnormally) a session with the processing device. However, in this embodiment, all changes occurring with the local credential store 425 are synchronized to the remote credential store 411 before the local credential store 425 is purged from the processing device. This particular embodiment may be especially useful when the principal 420 is accessing and creating an instance of the local credential store 425 from a processing device, such as a kiosk.

[0062] The distributed credential store 400 permits principals to have access to needed credentialing information from their local and personal computing environments at all times. Thus, a principal has needed credentialing information for interacting with another principal even when the principal falls out of direct communication with the identity service 410. The principal can re-synchronize with the remote credential store 411 when it re-establishes communication with the identity service 410 and communicates its synchronization policy. Any conflicts can be resolved by a global contract or global policy associated with a particular principal and maintained and managed by the identity service 410.

Claims

1. A computer-implemented method for managing a distributed credential store, comprising:

   associating (110) portions of an enterprise credential store to a principal credential store;
   selectively synchronizing (120) changes between the portions and the principal credential store; and
   managing (130) conflicts and the changes according to a policy.

2. The method of claim 1 wherein the associating further includes:

   aggregating (111) the portions from the enterprise credential store, wherein the portions are identified by the policy; and
   transmitting (112) the portions to a principal as an initial instance of the principal credential store.

3. The method of claim 1 further comprising:

   inserting (121) personal identity information into the principal credential store; and

EP 1560100A1 | >

preventing (122) the personal identity information from being synchronized with the enterprise credential store.

4. The method of claim 1 further comprising:

detecting (123) an insertion of new identity information into the principal credential store; and
updating (123) the enterprise credential store with the new identity information.

5. The method of claim 1 further comprising:

detecting (124) an insertion of new identity information into the enterprise credential store;
determining via the policy that the new identity information is included within the portions; and
updating (124) the principal credential store with the new identity information.

6. The method of claim 1 further comprising:

receiving (132) modifications to the policy from a principal; and
adjusting (132) the synchronization between the portions and the principal credential store based on the modifications.

7. The method of claim 1 further comprising using a trust specification (301) to ensure interactions between the entity credential store and the principal credential store are initially and remain trusted during the interactions.

8. A computer-implemented method for managing a distributed credential store, comprising:

establishing (210) a trust relationship with a remote credential store (303);
receiving (220) changes associated with one or more entries in the remote credential store into a local credential stor (302) ; and
transmitting (230) changes associated with one or more entries in the local credential store to the remote credential store.

9. The method of claim 8 further comprising maintaining (223) selective sets of the one or more entries within the local credential store (302) for separate unique principals (330).

10. The method of claim 8 further comprising identifying (224) for the remote credential store (303) the one or more entries in the remote credential store which are to be received as the changes.

11. The method of claim 10 further comprising managing (225) one or more personal identity information entries within the local credential store (302) which are not trans mitted as the changes associated with the one or more entries in the local credential store to the remote credential store (303).

12. The method of claim 8 further comprising managing (221) portions of the local credential store (302) from memory and managing other portions from storage.

13. The method of claim 8 further comprising managing (225) the trust relationship between the local credential store (302) and the remote credential store (303) using a trust specification (301).

14. The method of claim 8 further comprising managing (222) the received changes and the transmitted changes using a synchronization policy (310,320).

15. A computer-networked distributed credential management system (300), comprising:

a trust specification (301);
a local credential store (302); and
a remote credential store (303);

wherein the local credential store and the remote credential store interact with one another according to the trust specification, and wherein portions of the remote credential store are synchronized with portions of the local credential store, and vice versa.

16. The distributed credential management system of claim 15 further comprising a remote synchronization policy (320) that determines which of the portions of the remote credential store (303) are synchronized with the portions of the local credential store (302), and wherein the synchronization policy is accessible to the remote credential store.

17. The distributed credential management system of claim 16 further comprising a local synchronization policy (310) that determines which portions of the local credential store (302) are synchronized with the portions of the remote credential store (303).

18. The distributed credential management system of claim 16 wherein the remote synchronization policy (320) is defined by and modified by the local credential store (302).

19. The distributed credential management system of claim 15 wherein the local credential store (302) resides within a local processing environment of a principal (330).

20. The distributed credential management system of claim 15 wherein the local credential store (302) is managed by a policy and includes multiple records, wherein each record is associated with a different principal, and wherein each record is uniquely encrypted for each different principal.

21. A distributed credential store, residing in a computer- readable medium, the distributed credential store used to acquire credentialing information associated with a principal, the distributed credential store comprising:

a principal identifier field (401) capable of housing a principal identifier value that identifies a particular principal; and
a credentialing information record (402) associated with the principal identifier field and capable of housing credentialing information associated with the principal identifier value for the particular principal;

wherein the distributed credential store is initially generated by an identity service (410).

22. The distributed credential store of claim 21 the credential data store is maintained remotely by the identity service (410) and maintained locally by a principal service (420).

23. The distributed credential store of claim 22 wherein some portions of the credentialing information (402) which are maintained locally are not also maintained remotely.

24. The distributed credential store of claim 22 wherein portions of the credentialing information (402) which are synchronized and maintained both remotely and locally are defined by a policy which can be dynamically modified and initially set by the principal service (420).

25. The distributed credential store of claim 21 wherein the identity service (410) uses the principal identifier field (401) to construct multiple unique local credential stores (425), each unique local credential store associated with a unique instance of the distributed credential store.

26. The distributed credential store of claim 21 wherein the identity service (410) populates the credential information of the credential record (402) by aggregating identity information from one or more identity stores associated with the particular principal.

27. The distributed credential store of claim 21 wherein the identity service (410) and a principal service (420) cooperate to selectively synchronize portions of the credential information between one another.

28. A computer program product which when executing on a computer network performs the method of any one of claims 1 to 7 or claims 8 to 14.

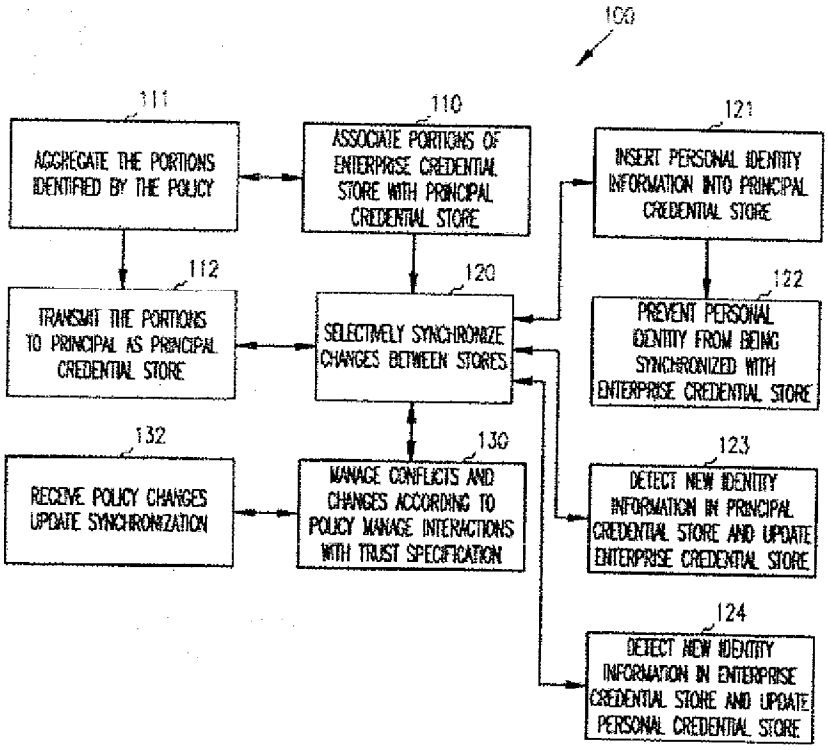

FIG. 1

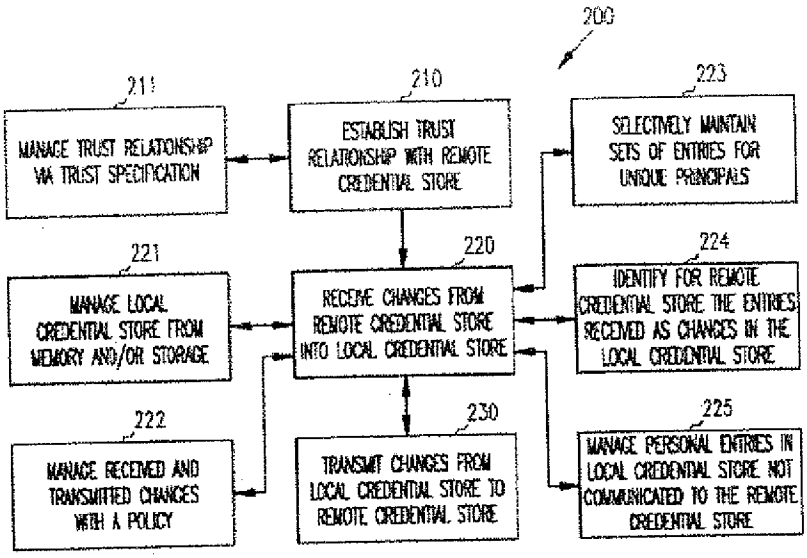
200
211
MANAGE TRUST RELATIONSHIP VIA TRUST SPECIFICATION
210
ESTABLISH TRUST RELATIONSHIP WITH REMOTE CREDENTIAL STORE
223
SELECTIVELY MAINTAIN SETS OF ENTRIES FOR UNIQUE PRINCIPALS
221
MANAGE LOCAL CREDENTIAL STORE FROM MEMORY AND/OR STORAGE
220
RECEIVE CHANGES FROM REMOTE CREDENTIAL STORE INTO LOCAL CREDENTIAL STORE
224
IDENTIFY FOR REMOTE CREDENTIAL STORE THE ENTRIES RECEIVED AS CHANGES IN THE LOCAL CREDENTIAL STORE
222
MANAGE RECEIVED AND TRANSMITTED CHANGES WITH A POLICY
230
TRANSMIT CHANGES FROM LOCAL CREDENTIAL STORE TO REMOTE CREDENTIAL STORE
225
MANAGE PERSONAL ENTRIES IN LOCAL CREDENTIAL STORE NOT COMMUNICATED TO THE REMOTE CREDENTIAL STORE

FIG. 2

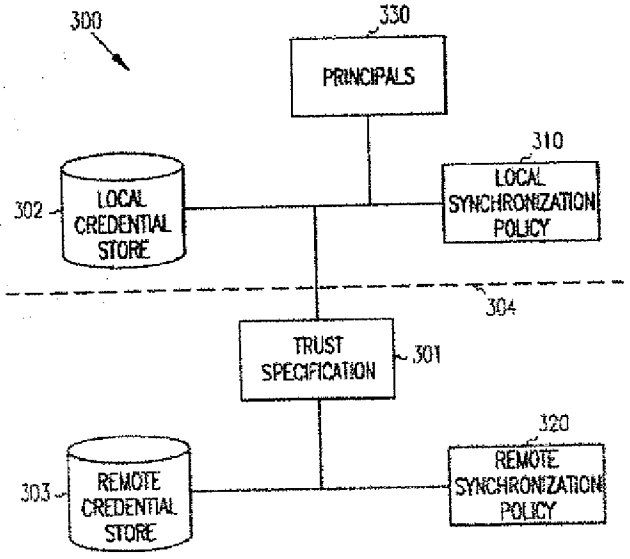
300
330
PRINCIPALS
310
LOCAL SYNCHRONIZATION POLICY
302
LOCAL CREDENTIAL STORE
304
TRUST SPECIFICATION
301
320
REMOTE SYNCHRONIZATION POLICY
303
REMOTE CREDENTIAL STORE

FIG. 3

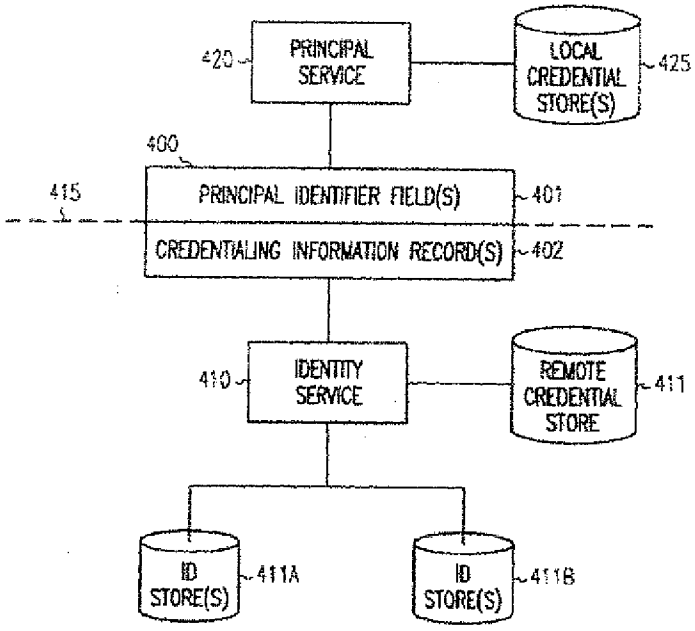

FIG. 4

European Patent Office

DECLARATION

which under Rule 45 of the European Patent Convention shall be considered, for the purposes of subsequent proceedings, as the European search report

Application Number EP 05 10 0336

The Search Division considers that the present application, does not comply with the provisions of the EPC to such an extent that it is not possible to carry out a meaningful search into the state of the art on the basis of all claims

Reason:

The claims relate to subject matter excluded from patentability under Art. 52(2) and (3) EPC. Given that the claims are formulated in terms of such subject matter or merely specify commonplace features relating to its technological implementation, the search examiner could not establish any technical problem which might potentially have required an inventive step to overcome. Hence it was not possible to carry out a meaningful search into the state of the art (Rule 45 EPC). See also Guidelines Part B Chapter VIII, 1-3.

The applicant's attention is drawn to the fact that a search may be carried out during examination following a declaration of no search under Rule 45 EPC, should the problems which led to the declaration being issued be overcome (see EPC Guideline C-VI, 8.5).

CLASSIFICATION OF THE APPLICATION (Int.Cl.7)

G06F1/00

Place of search	Date	Examiner
Munich	30 May 2005	Mezödi, S

EPO FORM 1504 (P04C37)